(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

PCT

(43) International Publication Date
8 November 2001 (08.11.2001)

(10) International Publication Number
WO 01/84768 A1

(51) International Patent Classification⁷: H04L 9/02

(21) International Application Number: PCT/US01/13444

(22) International Filing Date: 27 April 2001 (27.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/562,385 1 May 2000 (01.05.2000) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 09/562,385 (CON)
Filed on 1 May 2000 (01.05.2000)

(71) Applicant *(for all designated States except US)*: AUTHENEX, INC. [US/US]; 3031 Tisch Way, Suite 68, San Jose, CA 95128 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: LIN, Paul [US/US]; 1452 San Benito Drive, Fremont, CA 94539 (US).

(74) Agent: BEFFEL, Ernest, J., Jr.; Haynes & Beffel LLP, P.O. Box 366, Half Moon Bay, CA 94019 (US).

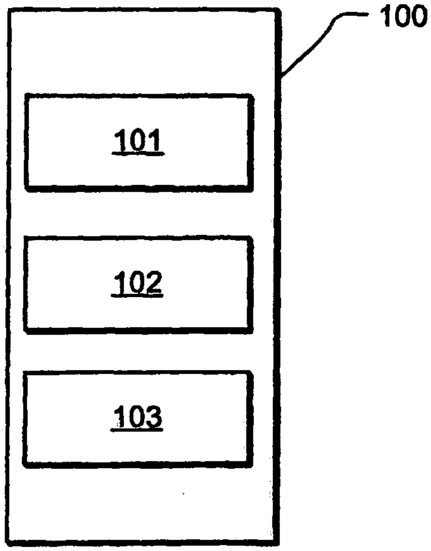
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD OF AUTHENTICATING USER



(57) Abstract: Authentication of a user is accomplished by an exchange including an electronic serial number, a plurality of substring designations, and a calculated authentication string. A user (210) and an authentication authority (212) each possess an identification string associated with the electronic serial number. By applying one or more operations, some of which may be exchanged across a network and others of which may be associated with the electronic serial number, a different authentication string can be calculated each time authentication is requested, making the methods and devices practicing this invention resistant to efforts to compromise the authentication.

METHOD OF AUTHENTICATING USER

Inventor: Paul Lin

BACKGROUND OF INVENTION

In our world of computer networks and electronic commerce, authentication of users and encryption of communications are critical concerns. One of the most widely used, standardized bases for user identification and encryption is a public key system. Users of the public key system are assigned a public key and a private key. The public key is published for use by others. The private key is installed by a user and not transmitted across a network, except, perhaps, when the private key is initially issued or installed. In the context e-mail, the installation typically associates the private key and an e-mail address. The installation process is somewhat cumbersome. The private key is not intended to be carried by the user from one machine to the next. It would be more desirable to develop a portable key system, which could be easily installed and carried by the user from one machine to the next, while retaining the characteristic that a critical secret, such as the private key, is never transmitted by the user.

A family of products for portable user identification are sold under the trademark ACTIVCARD. A smart card product is sold under the tradename ACTIVCARD GOLD. A keypad device requiring entry of a PIN is sold under the tradename ACTIVCARD ONE. Patents assigned to ACTIVCARD which potentially relate to the company's technology include U.S. Patent Nos. 5,937,068, 5,887,065, 5,802,176 and 5,737,421. As described on the company's web site, www.activcard.com/products/enduser, the smart card product is available with a reader and is compatible with any PC/SC smart card reader. The product is described on the web site as carrying on-board user data as well as identification and as being capable of being used for anything from opening doors to network user authentication. The corporate credentials which the web site says may be carried in the smart card include dynamic passwords, corporate digital signatures, static credentials and, at some time in the future, corporate electronic cash. Upon user entry of password or PIN, the smart card generates a dynamic password, a static password or a digital certificate. Again according to the web site, dynamic passwords may be generated either in accordance with an ActivCard-patented mechanism or the X9.9 standard. The battery may need to be changed every two years. The protocol for message exchanges between the smart card and server is not described on the company's web site. This is a relatively expensive system, designed for professional network administrator implementation. It is neither cheap nor easy to implement.

The second ACTIVCARD product has a key pad and LCD display. It is described on the web site as generating and displaying a dynamic password. The user transcribes the password from the LCD to a logon screen. Like the first product, it appears to be designed for professional network administrator implementation and may require a battery change after two years. If the battery wears down, the card may lose synchronization with the server and fail to generate appropriate time based passwords. It is relatively expensive, not easy to implement and taxing on the user to transcribe the password to the computer system. It would be more desirable to have an inexpensively manufactured, compact security device, which retains the characteristic that the authentication message which identifies the user is ever-changing. It would be further desirable to minimize the user's burden.

SUMMARY OF INVENTION

The present invention includes a device and method of authentication. In one embodiment, a key is provided containing logic and resources. The resources include an interface, a processor, and memory for processing logic, a password, an electronic serial number ("ESN") and an identification pad. The logic processes a password from the interface to make the key functional. The logic identifies the key by ESN. It receives a request to perform one or more authentication operations on one or more designated substrings and generates an authentication string. The authentication string is supplied to the interface. The ESN and authentication string can be transmitted simultaneously or in a sequence of ESN, request, authentication string.

Preferably, the ESN and identification pad are fixed in the key at manufacture. The logic and resources do not allow the key to modify the ESN or identification pad. The logic and resources do not allow access to the identification pad. One aspect of the invention may be that a confounding operation is fixed in the key at manufacture, which is applied to designated substrings under predetermined conditions.

The logic and resources may further include one or more timing delays. A password timing delay logic may introduce a first delay among a predetermined number of password entries and a second delay after the predetermined number of password entries, effectively slowing the processing of password entries. An authentication timing delay logic may introduce an authentication delay between password processing and request processing.

Another aspect of the key may include irretrievable password assignment. The logic and resources of the key may require a user to set a password, which is fixed in memory and not retrievable through the interface. Preferably, fixing of the password in memory is reported through the interface to activate the key. The logic and resources may not permit the password to be changed.

The logic may limit the allowable operations and substrings. It may require a plurality of operations. It may reject identity operations, such as add zero, multiply by one or logically "or" with a string of zeros.

A further embodiment of the present invention includes a key and terminal. The terminal may include a network connection. The interface of the key connects to the terminal, preferably by a USB connection. The key may control the terminal, either downloading program code, invoking native resources of the terminal or invoking special resources installed on the terminal to support the key. The key and terminal may initially require a user to set a password to activate the key. The terminal may announce activation of the key via its network connection, such as an Internet connection.

A key and terminal may be connected across a network with a initialization server. The logic and resources of the key may require an active connection between the terminal and initialization server in order to set a password and activate the key.

The terminal may include a transaction server. The terminal alternatively may be connected across a network with a transaction server. The transaction server may be a cash register, POS terminal, EC server, network server, or any other device requiring identification of a user. The transaction server may generate authentication operations and substring designations or may pass to the terminal operations and designations from another source.

An authentication system may include a key, terminal, transaction server and authentication server. The transaction server may be incorporated in the terminal or connected across a network. The transaction server is preferably connected by a trusted connection to the authentication server. This trusted connection may be a physically secure connection, such as a local bus or local area network, an encrypted connection, such as a virtual private network, an authenticated connection with digitally signed messages, or any other trustworthy connection. The terminal may be in communication only with the transaction server or with both the transaction and authentication servers. The authentication server includes a table of ESNs and identification pads.

An authentication server may practice the present invention. The authentication server may include resources and logic to interact with a user system and authenticate a user. The resources may include an interface, a processor, memory for processing logic and for a table of ESNs and identification pads. The logic processes an ESN from the interface, designates one or more substrings, specifies a set of operations on one or more designated substrings to the interface, receives an authentication string from the interface, and determines whether the response is authentic. The logic may determine whether the ESN is currently valid, before proceeding with authentication. It may implement a delay or lockout based on unsuccessful authentication requests.

An authentication server may be accessible only through a trusted connection or it may receive authentication requests across an insecure network from an unauthenticated source. The authentication server may generate an authentication by any secure protocol.

The present invention alternatively can be summarized from the claims. One device practicing the present invention is an authentication key including a processor, input/output interface(s), an electronic serial number and identification string accessible to the processor, and logic utilizing the processor to receive substring designations in response to identifying itself with an electronic serial number, to calculate the result of performing one or more operations applying the substring designations to the identification string, and to output the result. One aspect of the present invention is that the processor, electronic serial number and identification string should be embedded on a single chip or located on a single set semiconductor substrate, for security reasons. The form factor of an authentication key may be that of a standard credit card or a smaller form factor suitable to be attached to a key ring. The operations applied to the substring designations may be any operation, such as addition, subtraction, multiplication, division or logical operations such as an exclusive or. These operations may be embedded in the device or may be received from an outside source, or some combination of the two. The logic utilizing the processor may provide security services, such is requiring a password to be set initially and entered each time the device is used. Setting the password may be limited to circumstances when the device is in communication with an initialization server which activates the authentication key. The logic to set a password may prevent password from being changed, accessed or recovered once it is set. The logic utilizing the processor should prevent recovery of our access to the embedded identification string.

An additional device practicing the present invention may comprise a terminal connected to a network, an authentication key including a processor, an electronic serial number and identification string and logic utilizing the processor. The logic may receive a plurality of substring designations in response to identifying itself with an electronic serial number. It may calculate a result of performing one or more operations applying the substring designations to the identification string, and may communicate with the terminal utilizing a universal serial bus protocol. Additional aspects of this authentication subsystem may incorporate the same features as incorporated in an authentication key.

A method practicing the present invention, utilizing an electronic serial number and identification string, may include the steps of transmitting an electronic serial number, receiving a plurality of substring designations, applying one or more operations to the designated substrings to calculate a result, and transmitting the result. An additional aspect of this method may include receiving one or more operation designations and applying combination of received operation designations and embedded operation designations to calculate a result. The method may include providing security services, such as requiring a password to be set initially and entered each time each time authentication is requested. Setting the password may be limited to circumstances when there are active communications between a client hand and initialization server.

A transaction server in communication with a client and with an authorization server also may practice the present invention. Such a transaction server may include a processor and logic utilizing the processor to receive and recognize an electronic serial number and forward that electronic serial number from the client to the authorization server, to forward a plurality of substring designations from the server to the client, to forwarding an authentication string from the client to the server, and to receive authorization from the server, based on successful authentication. The transaction server also may forward one or more operation designations, in addition to forwarding a plurality of substring designations.

An additional method practicing the present invention may include the steps of receiving and recognizing and electronic serial number from a client and forwarding that serial number to a server, forwarding a plurality of substring designations from the server to the client, forwarding an authentication string from client to a server, and receiving an authorization without server. This method may also included forwarding one or more operation designations, in addition to forwarding a plurality of substring designations.

An authentication server may also practice the present invention. An authentication server may comprise a processor with input/output interface(s), a list of record electronic serial numbers and record identification strings and logic utilizing the processor. The logic may be adapted to receive a particular electronic serial number, select and send one or more operation designations, receive an authentication string, and compare the authentication string to a result calculated by applying the one or more operations to the plurality of designated substrings of the record identification string. An aspect of the logic utilizing the processor may be that selects and sends operations to perform on the designated substrings. These designated operations may be combined with one or more confounding operations to calculate the result.

A method specially adapted to be used by an authentication server may utilize a list of record electronic serial numbers and record identification strings. It may include the steps of receiving a particular electronic serial number, selecting and sending a plurality of substring designations, receiving an authentication string, applying one or more operations to the designated substrings, and comparing the authentication string to the result of the operations. One aspect of present invention may be that the authentication server selects and sends operation designations which are subsequently used to calculate a record result. A combination of designated operations sent and embedded confounding operations not sent as part of the method may be applied to the designated substrings the calculate the record result.

An overall authentication system practicing the present invention may include an authorization server, a transaction server having a trusted link with the authorization server and an authentication key in communication with the transaction server. The authorization server in this embodiment of the present invention may include a list of record electronic serial numbers and record identification strings and logic to input an electronic serial number, select and output a plurality of substring designations, input an authentication string, calculate a record result of performing one or more operations on the designated substrings, and compare the authentication string to the record result. The transaction server in this embodiment of the present invention may include logic to forward the electronic serial number to the authorization server, forward a plurality of substring designations from the authorization server, forward the authorization string to the authorization server and receive a successful authentication message from the authentication server. An authentication key in this embodiment of the present invention may include an electronic serial number, an identification string, and logic to output the electronic serial number, input a plurality of substring designations, calculate the authentication string, and output the authentication string. Each of the components of this overall authentication system may include a processor. The logic and each of the components may utilize the processor and may be in communication with one or more processors of the other components.

An overall method practicing the present invention may include the steps of sending a particular electronic serial number from a client to a server, sending a plurality of substring designations from the server to the client, applying one or more operations to the designated substrings to calculate an authentication string, sending the authentication string from the client to the server, applying one or more operations to the designated substrings of the record identification string to calculate a record result, and comparing the authentication string and the record result. In this embodiment, calculations may take place in any sequence or concurrently on the client and the server. It is not necessary for the server to wait to receive an authentication string, before applying operations to the record identification string to calculate a record result. One aspect of the present invention may be that the server selects and sends operation designations which are subsequently used to calculate results in record in the. A combination of designated operations sent and embedded confounding operations not sent as part of the method may be applied to the designated substrings to calculate results.

DESCRIPTION OF THE FIGURES

Figure 1 is a block diagram of a client or authentication key.

Figure 2 depicts a method practiced using a client, such as an authentication key, to generate an authentication string in response to substring designations.

Figure 3 is block diagram of an authentication subsystem comprising an authentication key and a terminal in communication with a network.

Figure 4 he is a the block diagram of a transaction server linked to a client and an authentication server.

Figure 5 depicts a message forwarding protocol practiced by a transaction server in accordance with the present invention.

Figure 6 is a block diagram of an authentication server.

Figure 7 depicts a protocol for selecting and sending substring designations and for verifying an authentication string received from a client.

Figure 8 depicts an authentication system comprising a client, a transaction server and an authentication server.

Figure 8 depicts a protocol for authentication, including messages exchanged between a client and server and string operations performed by the client and server.

DETAILED DESCRIPTION

The following detailed description is made with reference to the figures. Preferred embodiments are described to illustrate the present invention, not limit its scope, which is defined by the claims. Those of ordinary skill in the art will recognize a variety of equivalent variations on the description that follows.

Figure 1 illustrates a device embodying the present invention which is useful for user identification or authentication and for encryption. This device is capable of producing an authentication string, which varies from one use to the next. The entire device 100, which may be described as authentication key, may match the form factor of standard credit card or may be smaller and adapted to be attached to a key ring, for instance. The device will have one or more interfaces 101 which support input and output. The device will have a processor and logic utilizing the processor 102. Embedded in the device and accessible to the processor will be an electronic serial number and identification string 103. The electronic serial number and identification string will be assigned to device before the typical user receives the authentication key. The particular electronic serial number and identification string will be recorded at the time they are assigned. An authority, such as a licensor, licensee, manufacturer or distributor of the authentication key will maintain a list of record electronic serial numbers and record identification strings. The electronic serial numbers preferably are unique, as are the combinations of electronic serial numbers and identification strings. The identification strings preferably are long, so that numerous substrings can be selected without being reused. For instance, an identification string with 10,000 positions may be used. Each of the positions may be either a binary digit, hexadecimal number, ASCII character or any other symbol. The logic utilizing the processor allows the authentication key to output an electronic serial number, input a plurality of substring designations applicable to the identification string, calculate a result of performing one or more operations using the designated substrings of the identification string, and output the result has an authentication string. The operations to calculate a result may be any conventional string operation, such as addition, multiplication, subtraction, division or logical operations such as an XOR. A further aspect of the present invention may be that the logic receives as input one or more operators to apply to the designated substrings. In addition to receiving operators to apply, the authentication key may contain one or more confounding operations, which will be assigned at the same time as the electronic serial number and identification string. The authority that maintains the list of record electronic serial numbers and identification strings will also maintain a list of record confounding operations. In case one or more operations are received by the authentication key across an insecure network, the additional presence of confounding operations will enhance security. The presence of confounding operations also will tend to defeat systematic efforts to reverse engineer and identification string in order to set up a series of parallel equations. Assuming that substring designations are rarely repeated, the authentication key and related components will frustrate attempts by a person who intercepts packets and impede their efforts to reverse engineer the identification string.

One aspect of authentication key may be that the processor, logic, electronic serial number and identification string are all embedded in a single chip or logical device or located on a single semiconductor substrate. The advantages of a single chip include reduced manufacturing costs and reduced accessibility to logic probes or other means of extracting the password or identification string from the authentication key.

Another aspect of the authentication key may be that it includes logic to require entry of a password each time an authentication or encryption session is initiated. This password may be assigned at the same time as electronic serial number and supplied to the user or, preferably, it may be set by the user in order to activate the authentication key. The logic for setting a password may be operative only when there is communication through the interface from the authentication key to an initialization server which includes a list of record electronic serial numbers. The initialization server may include logic to verify that an authorization key corresponding to a particular electronic serial number is eligible for activation. It may verify that the electronic serial number has not previously been reported as lost or stolen or otherwise deactivated. It also may determine that the electronic serial number has been properly assigned to an individual and that individual has acknowledged receipt of the authorization key. Logic implementing password protection and requiring entry of a password may include one or more delays after an unsuccessful password entry attempt. The delay after one or two unsuccessful entries may be relatively brief. A longer delay take effect after several unsuccessful password entries. The effect of introducing delays is to frustrate systematic attempts to defeat password protection. The logic related to password protection may further prevent the password from being changed once it has been set. This feature may be implemented either in software, as my setting a nonvolatile bit in memory, or in hardware, as by burning a key is in the logic when a password is entered. The password-related logic should further prevent access to or recovery of the password from the authorization key. This is a desirable feature because in authorization key can be manufactured at a low cost, making it reasonable to replace an authorization key instead of recovering a forgotten or lost password. The logic utilizing the processor preferably will also prevent access to the identification string.

Figure 2 illustrates a method of user authentication utilizing an electronic serial number and identification string which practices the present invention. This figure illustrates communications between the authentication key or client 210 and a server such as an identification or authentication server 212. In this aspect of the present invention, the client will transmit an electronic serial number 214 and wait for response. It deletes next word will may receive a plurality of substring designations applicable to an embedded identification string 216. One or more operations may be performed on the designated substrings of the embedded identification string to calculate a result. The result is then transmitted 218. Another aspect of this method may be that one or more operations are received to be used in to calculate the result, in addition to receiving the substring designations. The method may further require a user to enter a password before receiving substring designations and may require the user to set the password in order to activate the authentication key. Preferably, the user would be required to set a password while in the late next word line communication with an initialization server. Another aspect of this method may be that calculating a result involves applying one or more confounding operations which are neither sent nor received as part of the method. Combinations of confounding operations and designated operations received may be applied to calculate the result.

Figure 3 depicts using an authorization key in conjunction with a terminal, such as a personal computer 326. The authorization key 100 and its components 102 and 103, are generally as depicted in figure 1. The authorization key is preferably as connected to the terminal utilizing a universal serial bus (USB) protocol or the equivalent 325. The terminal, in turn, is connected to a network 327, which may be a local area network, the Internet or any other network. Advantages of utilizing the USB protocol, as opposed to a lesser about equivalent protocol, may include supplying power to the authentication key and supporting communication between the authorization key and the late next word with the terminal without a separate step of installing especially adapted software on the late next two characters to the terminal.

Many aspects of the authorization subsystem overlap with aspects of the authorization key. The logic may support inputting designations of one or more operations to be performed, requiring password entry, implementing delays after unsuccessful password entry, and requiring the user to set a password, preferably while in communication with an initialization server. The logic may further prevent a password from being changed, recovered or accessed once it is set. It should prevent recovery of or access to the identification string. It may include one or more confounding operations which may be applied separately or in combination with designated operations. A method implementing the present invention on authentication subsystem comprising authentication key and a terminal may closely resemble a method utilizing only an authentication key.

Figure 4 illustrates a transaction server 430 which may sit between authentication key or authentication subsystem 400 and an identification or authentication server 440. The transaction server 430 is in communication with the authentication key 400. This communication may be across the network, a universal serial bus or any other conduit for electronic communications. The transaction server 430 may be widely separated from the authentication key 400, as would be expected in electronic commerce setting or a worldwide computer network requiring authentication when a user logs on. Alternatively, the transaction server may be embedded in point-of-sale terminal, a cash register, an ATM, or other device which physically connects with the authentication key. The authentication server 430 will include a processor and logic utilizing the processor 432. This logic will receive and recognize electronic serial number from a client and forward electronic serial number to an authentication server. It will forward a plurality of substring designations for the authentication server to the client. It will forward an authentication string from the client to the authentication server. From the authentication server, it will receive an indication of whether the client passes or fails authentication. The authentication server will determine whether the client passes authentication by comparing the forwarded authentication string with a record result calculated by applying certain operations to the designated substrings of a record identification string. The record identification string will correspond to a record serial number matching the forwarded electronic serial number. An aspect of the transaction server may be that it forwards designations of one or more operations to perform on designated substrings, in addition to forwarding the substring designations.

Figure 5 illustrates a method of obtaining client authentication, from the perspective of the transaction server. This figure depicts the client 550, a transaction server 551, and an authentication server 552. The process begins with the transaction server receiving and recognizing an electronic serial number from client 554. The electronic serial number is forwarded to an authentication server. If necessary, the transaction server determines which of a plurality identification servers should receive the electronic serial number. The transaction server receives and forwards to the client a plurality of substring designations 556 applicable to an identification string which is known to the client and the authentication server. The substring designations are forwarded from the server to the client. The identification string to which these designations apply his unknown to the transaction server and not transmitted. The client responds to the forwarded substring designations by calculating an authentication string. The transaction server forwards an authentication string from the client to the authentication server 557 and awaits an indication from the authentication server 558 as to whether the client has passed or failed authentication. A further aspect of this method may be the transaction server forwards designations of one or more operations to perform on designated substrings, in addition to forwarding the substring designations.

Figure 6 is a block diagram of an authentication server 600. The authentication server comprises an interface for receiving input and transmitting output 601, a processor and logic utilizing the processor 602, and a list of record electronic serial numbers and identification strings 603 accessible to the processor. The interface may utilize one or more ports. It may connect the server to a local area network, the Internet, a virtual private network, a private network or virtually any communication channel. The logic utilizing the processor will be adapted to receive an electronic serial number, select and transmit a plurality of substring designations, receive an authentication string and compare the authentication string to a result calculated by applying the one or more operations to the plurality of designated substrings. These designated substrings apply to a record identification string having a record serial number corresponding to the received electronic serial number. This record identification string is the same as a record identification string known to a device which transmitted its electronic serial number. When the authentication string and the calculated result based on the record identification string match, the authentication server may announce a successful authentication. A further aspect of the authentication server may be that its selects and transmits designations of one or more operations to perform using designated substrings. In addition to these designated operations, an authentication server may further include a list of record confounding operations to be applied to designated substrings. These confounding operations will correspond to confounding operations known to the device which transmitted its electronic serial number. The logic to calculate a result may apply a combination of confounding operations and designated operations.

Figure 7 depicts a method of user authentication by an authentication server utilizing a list of record electronic serial numbers and record identification strings. The client or authentication key 710 works in conjunction with the authentication server 712. The authentication server receives a particular electronic serial number 714. Its selects and sends a plurality of substring designations 716. It receives an authentication string 718. It applies one or more operations to designated substrings of a record identification string. The record identification string corresponds to the particular electronic serial number received. The authorization server calculates a record result and compares the record result to the authentication string. The authorization server indicates the success or failure of the authentication 720. As with other aspects of the present invention, this method may involve selecting and sending one or more operations designations which are later used by the authorization server in the applying step. These operation designations are also used by the client to prepare an authentication string which is received by the authentication server. This method also may involve use of one or more record confounding operations, either by themselves or in conjunction with designated operations.

Figure 8 depicts an overall authentication system, including an identification or authentication server 600, a transaction server 430 and an authentication key 100. The authentication server and transaction server are in communication with each other, preferably across a trusted link. The transaction server and authentication key are in communication with each other, although the link need not be trusted. The transaction server authentication server may be part of the same device or server, in which case the trusted link may be an electronic bus. Alternatively, the authentication server and transaction server may be widely dispersed, as will be the case when a bank operates the authentication server and a number of electronic commerce businesses operate transaction servers. A trusted link may be physically secure, digitally signed, encrypted, via a virtual public network or any other secure, trustworthy link. Security risks are minimized when the authentication server and transaction server can trust that the information they exchange is authentic. The authentication server 600, transaction server 430 and authentication key 100 may include many of the same components as depicted in the figures 6, 4 and 1, and are numbered accordingly.

Figure 9 depicts an overall method of user authentication, including steps carried out at both the client and the server. The client or authentication key 910 is in communication with the server, which may be referred to as an identification or authentication server 912. The client sends a particular electronic serial number to the server 914. The server selects and sends a plurality of substring designations to the client 916. The client applies the one or more operations to the designated substrings of a particular identification string known to the client 917. It calculates an authentication string which it sends the server 918. The server applies the same one or more operations as applied by the client to the designated substrings of a record identification string known to the server 919. The record identification string corresponds to the particular identification string, according to the particular electronic serial number. The server calculates a record result and compares the application string to this result. The authentication server may then report whether the client has passed or failed authentication 920. A further aspect of this overall method may be that designated operations are selected and sent from the server to the client, along with designated substrings. Designated operations may be combined with confounding operations which are known to the client and retrievable by the server based on the particular electronic serial number sent by the client.

The present invention may be applied in a wide variety of circumstances. Authentication of users is essential to preventing credit card fraud in electronic commerce transactions. Some sources indicate that credit card fraud in electronic commerce may be as high as 18 percent. Accordingly, companies which assure payment from online credit card transactions charge businesses a hefty premium. The present invention may reduce the premium. It also may allow an authentication server to transmit credit card information directly to a transaction server, in connection with indicating that the user has passed authentication. If the user has more than one credit card, the user may be allowed to select the credit card which the authentication server reveals to the transaction server, preferably via a trusted communication channel. A combination of user authentication and delivery of credit card information from a trusted source will facilitate electronic commerce.

The present invention also can function has a membership ID card. For online sites, such as bookstores and online entertainment, as user can be authenticated. When user anonymity is desired, an authentication server coupled with a deposit account or other credit mechanism can combine anonymous authentication of the user and assured payment for goods and services. The present invention can be used to authenticate the user and implement a payment forwarding system, without revealing the user's name. An embodiment of the present invention also can function has a pass key, when a membership ID card is used the gain entrance to the facility. Each authentication key would serve as a unique ID card which could not be duplicated or forged.

Online banking is a further application for the present invention. An authentication key or method embodying the present invention would serve as the Web equivalent of a driver's license. It would be more secure than an ATM card, because it could not readily be duplicated or forged. In cooperation with an authentication authority, one authentication key could be used for banking and for electronic commerce or other functions.

An authentication key or method practicing the present invention could be used in conjunction with authentication server to generate prepaid online tokens. A deposit account or other credit mechanism accessible by the authentication server could be debited to create an online token, after carrying out an authentication process.

In the realm of business to business transactions, an authentication key or method embodying the present invention can create trust and security on a communications link which is otherwise insecure.

Computer network users can benefit from an authentication key or method embodying the present invention. A network server could allow access privileges to users based on authentication in accordance with the present invention. A user carrying an authentication key could be granted the same privileges for network access at any terminal which they accessed.

The present invention also can be applied to e-mail, to assure that the person reading and e-mail is the intended recipient. In this application, either the delivery or decryption of e-mail could be controlled based on user authentication in accordance with the present invention. The authentication server could control the release of e-mail or viewing of e-mail. The authentication server also could provide an e-mail application with a token or encryption string to enable a user to read a particular e-mail message or to access and e-mail account.

Those having skill in the field of security will also realize that the authentication string generated by the present invention can also be used as a basis for encryption. Instead of transmitting an authentication string across the network, a client could generate an authentication string, say 128 bits long, and use than string as a basis for encryption. A string for encryption purposes can be generated and used in lieu of authentication or in addition to authentication. The same steps described above of transmitting an electronic serial number, receiving a plurality of substring designations and, optionally, operation designations, and applying operations to the designated substrings could be used to generate an authentication string for encryption purposes. An authentication string generated for encryption purposes would, of course, not be transmitted across a network.

This list is intended to indicate a variety environments in which the present invention would have practical application. This list of environments is not tended to limit the scope of the invention.

The present invention may realize a variety of advantages over prior technology. The present invention facilitates issuance of authorization keys which can authenticate a user independent of where they are or what terminal they are using. The user can be authenticated and a terminal in their home, their office, or a facility that they are visiting. The present invention can be practiced using an inexpensive custom chip and plastic card, for instance in the form factor of an ordinary credit card. Such cards could be manufactured and registered with an authentication authority for less than five dollars each. The present invention generates an ever-changing authentication string which cannot be intercepted and misused. The ever-changing authentication string cannot readily be forged, because of security mechanisms provided to defeat access to the embedded identification string from which the authentication string is derived. The embedded identification string is never transmitted across a network which may potentially be compromised. An authentication key practicing the present invention would be very convenient for a user. Utilizing a universal serial bus, an authentication key could communicate with existing personal computers without any need to install special software on the personal computers. It could take advantage of the plug and play capabilities now available in many personal computers. A device embodying the present invention would be easier to use than some other devices, such as the previously mentioned time-based device, from which a user must read an authentication code before time passes and a new authentication code is generated by the device. Additional advantages of the present invention will be apparent to those skilled in the art.

While the present invention is disclosed by reference to the preferred embodiments and examples detailed above, it is to be understood that these examples are intended in an illustrative rather than in a limiting sense. It is contemplated that modifications and combinations will readily occur to those skilled in the art, which modifications and combinations will be within the spirit of the invention and the scope of the following claims.

CLAIMS

What is claimed is:

1. An authentication key, including:

(a) a processor with one or more input/output interfaces;

(b) an electronic serial number and an identification string accessible to the processor;

(c) logic utilizing the processor to

output the electronic serial number;

input a plurality of substring designations;

calculate a result of performing one or more operations using the designated substrings of the identification string; and

output the result.

2. The authentication key of claim 1, wherein the processor, the logic utilizing the processor, the electronic serial number and the identification string are located on a single semiconductor substrate.

3. The authentication key of claim 1, wherein the processor, the logic utilizing the processor, the electronic serial number and the identification string are embedded in a single chip.

4. The authentication key of claim 1, wherein a form factor of the authentication key matches a standard credit card.

5. The authentication key of claim 1, wherein the logic to calculate a result adds together designated substrings.

6. The authentication key of claim 1, wherein the logic to calculate a result multiplies together designated substrings.

7. The authentication key of claim 1, wherein the logic to calculate a result calculates

a difference of designated substrings.

8. The authentication key of claim 1, wherein the logic to calculate a result calculates a quotient of designated substrings.

9. The authentication key of claim 1, wherein the logic to calculate a result calculates a logical XOR of designated substrings.

10. The authentication key of claim 1, wherein the logic to input a plurality of substring designations further includes logic to input designations of one or more operations to perform.

11. The authentication key of claim 1, further including logic to require entry of a password prior to transmitting the electronic serial number.

12. The authentication key of claim 11, wherein the logic to require entry of a password includes one or more delays after unsuccessful entry of a password.

13. The authentication key of claim 1, further including logic to set a password.

14. The authentication key of claim 13, wherein the logic to set a password is operative only when the interface is in communication with an initialization server which includes a list of electronic serial numbers.

15. The authentication key of claim 13, wherein the logic to set a password further includes logic to prevent the password from being changed.

16. The authentication key of claim 13, wherein the logic to set a password further includes logic to prevent recovery of the password.

17. The authentication key of claim 13, wherein the logic to set a password further includes logic to prevent access to the password.

18. The authentication key of claim 1, further including logic to prevent recovery of the identification string.

19. The authentication key of claim 1, further including logic to prevent access to the identification string.

20. The authentication key of claim 1, further including one or more confounding operations and the logic to calculate a result applies the confounding operations to one or more of the designated substrings.

21. The authentication key of claim 1, further including one or more confounding operations and the logic to calculate a result applies the designated operations and the confounding operations to the designated substrings.

22. An authentication subsystem, including:

(a) a terminal connected to a network;

(b) an authentication key including a processor, an electronic serial number, and an identification string accessible to the processor, and logic utilizing the processor to

output the electronic serial number;

input a plurality of substring designations;

calculate a result of performing one or more operations using the designated substrings of the identification string; and

communicate with the terminal;

wherein the authentication key is connected to the terminal utilizing a Universal Serial Bus protocol.

23. The authentication subsystem of claim 22, wherein the logic to input a plurality of substring designations further includes logic to input designations of one or more operations to perform.

24. The authentication subsystem of claim 22, further including logic to require entry of a password prior to transmitting the electronic serial number.

25. The authentication subsystem of claim 24, wherein the logic to require entry of a password includes one or more delays after unsuccessful entry of a password.

26. The authentication subsystem of claim 22, further including logic to set a password.

27. The authentication subsystem of claim 26, wherein the logic to set a password is operative only when the interface is in communication with an initialization server which includes a list of electronic serial numbers.

28. The authentication subsystem of claim 26, wherein the logic to set a password further includes logic to prevent the password from being changed.

29. The authentication subsystem of claim 26, wherein the logic to set a password further includes logic to prevent recovery of the password.

30. The authentication subsystem of claim 26, wherein the logic to set a password further includes logic to prevent access to the password.

31. The authentication subsystem of claim 22, further including logic to prevent recovery of the identification string.

32. The authentication subsystem of claim 22, further including logic to prevent access to the identification string.

33. The authentication subsystem of claim 22, further including one or more confounding operations accessible to the processor and the logic to calculate a result

applies the confounding operations to one or more of the designated substrings.

34. The authentication subsystem of claim 22, further including one or more confounding operations accessible to the processor and the logic to calculate a result applies the designated operations and the confounding operations to the designated substrings.

35. A method of user authentication utilizing an electronic serial number and an identification string, including the steps of:

(a) transmitting the electronic serial number;

(b) receiving a plurality of substring designations applicable to the identification string;

(c) applying one or more operations to the designated substrings to calculate a result; and

(d) transmitting the result.

36. The method of claim 35, wherein the receiving step further includes receiving one or more operation designations for the applying step.

37. The method of claim 35, further including the step of requiring the user to enter a password before receiving the plurality of substring designations.

38. The method of claim 37, further including the step of requiring the user to set a password.

39. The method of claim 37, further including the step of requiring the user to set a password which cannot be recovered.

40. The method of claim 37, further including the step of requiring the user to set a password, while in communication with an initialization server.

41. The method of claim 35, utilizing one or more confounding operations, wherein the applying step applies the confounding operations to the designated substrings.

42. The method of claim 41, wherein the receiving step further includes receiving one or more operation designations and the applying step applies the designated operations and the confounding operations to the designated substrings.

43. A transaction server in communication with a client and an authorization server, including:

(a) a processor; and

(b) logic utilizing the processor to

receive and recognize an electronic serial number from the client and forward the electronic serial number to the authorization server;

forward a plurality of substring designations from the authorization server to the client;

forward an authentication string from the client to the authorization server;

receive from the authorization server an indication of whether the client passes authentication.

44. The transaction server of claim 43, wherein the logic to forward substring designations further includes logic to forward designations of one or more operations to perform on the designated substrings.

45. A method of obtaining client authentication, including the steps of:

(a) receiving and recognizing an electronic serial number from a client and forwarding the electronic serial number to an authorization server;

(b) forwarding a plurality of substring designations applicable to an identification string known to the client and the authorization server, from the authorization server to the client;

(c) forwarding an authentication string from the client to the authorization server;

(d) receiving from the authorization server an indication of authentication of the client.

46. The method of obtaining client authentication of claim 45, wherein the step of forwarding substring designations further includes forwarding one or more operations to perform on the designated substrings.

47. An authentication server, including:

(a) a processor with an interface for receiving input and transmitting output;

(b) a list of record electronic serial numbers and record identification strings accessible to the processor;

(c) logic utilizing the processor to

receive an electronic serial number;

select and transmit a plurality of substring designations;

receive an authentication string; and

compare the authentication string to a result calculated by applying one or more operations to the plurality of designated substrings.

48. The authentication server of claim 47, wherein the logic to input a plurality of substring designations further includes logic to select and transmit designations of one or more operations to perform.

49. The authentication server of claim 47, further including one or more record confounding operations and the logic to calculate a result applies the confounding operations to one or more of the designated substrings.

50. The authentication server of claim 47, further including one or more record confounding operations and the logic to calculate a result applies the designated operations and the confounding operations to the designated substrings.

51. A method of user authentication utilizing a list of record electronic serial numbers and record identification strings, including the steps of:

(a) receiving a particular electronic serial number;
(b) selecting and sending a plurality of substring designations;
(c) receiving an authentication string;
(d) applying one or more operations to the designated substrings of record identification string corresponding to the particular electronic serial number to calculate a record result; and
(e) comparing the authentication string and the record result.

52. The method of claim 51, wherein the selecting and sending step further includes selecting and sending one or more operation designations which are used in the applying step.

53. The method of claim 51, utilizing one or more record confounding operations corresponding to the particular electronic serial number, wherein the applying step applies the confounding operations to the designated substrings.

54. The method of claim 53, wherein the selecting and sending step further includes selecting and sending one or more operation designations and the applying step applies the designated operations and the confounding operations to the designated substrings.

55. An authentication system, including:
(a) an authorization server including a list of record electronic serial numbers and record identification strings and logic to

input a particular electronic serial number;

select and output a plurality of substring designations;

input an authentication string;

calculate a record result of performing one or more operations using the designated substrings of the record identification string;

compare the authentication string to the record result;

(b) a transaction server having a trusted link with the authorization server including logic to

forward the particular electronic serial number to the authorization server;

forward the plurality of substring designations from an authorization server;

forward the authentication string to the authorization server;

receive from the authorization server an indication of the result of comparing the authentication string to the record result;

(c) an authentication key in communication with the transaction server, including the particular electronic serial number, an identification string and logic to

output the particular electronic serial number;

input the plurality of substring designations;

calculate the authentication string as result of performing one or more operations using the designated substrings of the identification string;

output the authentication string.

56. A method of user authentication, including the steps of:

(a) sending a particular electronic serial number from a client to a server;

(b) sending a plurality of substring designations from the server to the client;

(c) applying one or more operations to the designated substrings of a particular identification string to calculate an authentication string;

(d) sending the authentication string from the client to the server;

(e) applying the one or more operations to the designated substrings of a record identification string to calculate a record result; and

(f) comparing the authentication string and the record result.

57. The method of claim 56, further including the step of sending designations of one or more operations to perform on the designated substrings from the server to the client.

58. The method of claim 56, utilizing one or more record confounding operations corresponding to the particular electronic serial number, wherein the applying step applies the confounding operations to the designated substrings.

59. The method of claim 58, wherein the selecting and sending step further includes selecting and sending one or more operation designations and the applying step applies the designated operations and the confounding operations to the designated substrings.

Fig. 1

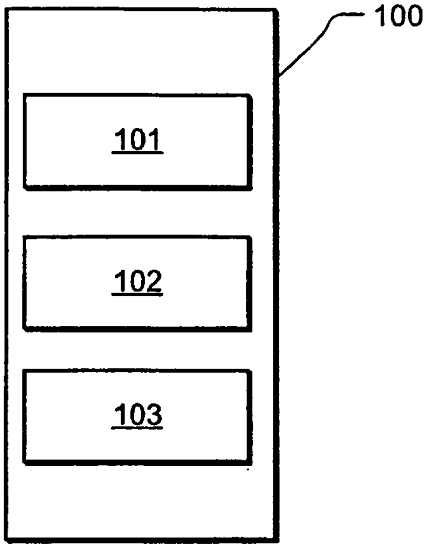


Fig. 2

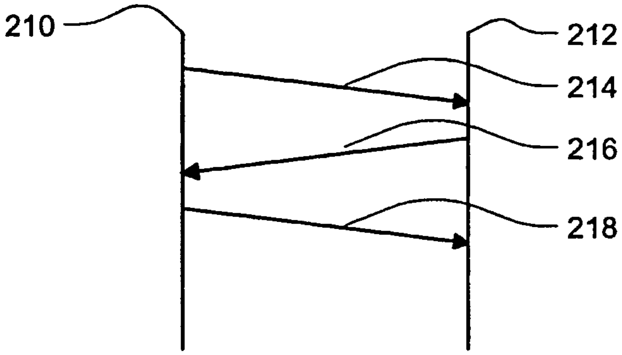


Fig. 3

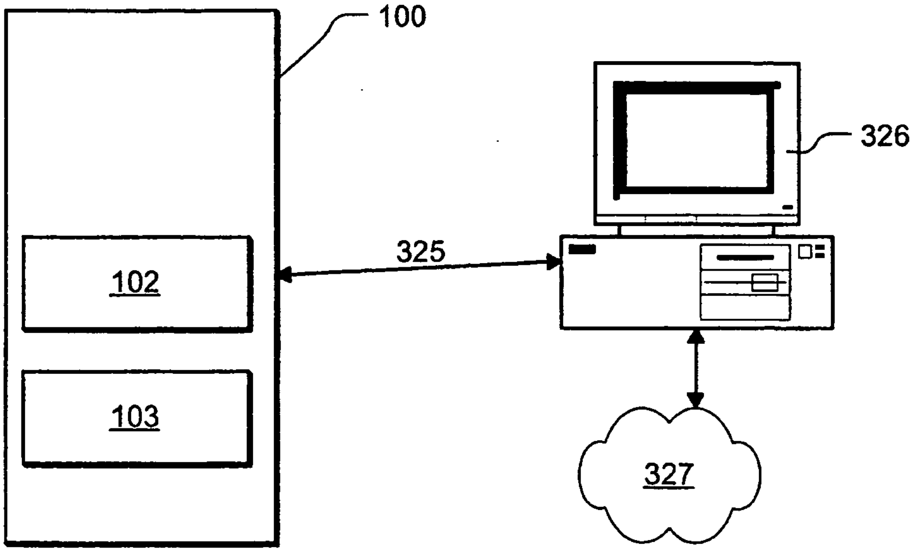


Fig. 4

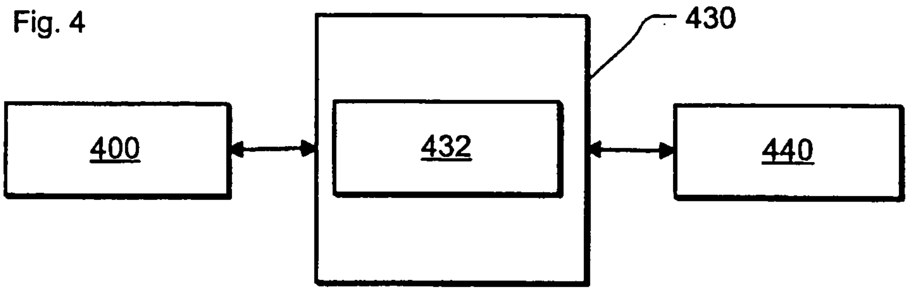


Fig. 5

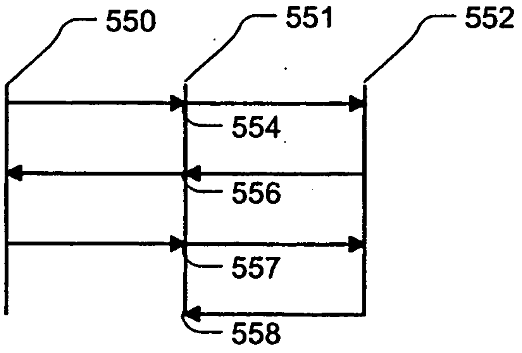


Fig. 6

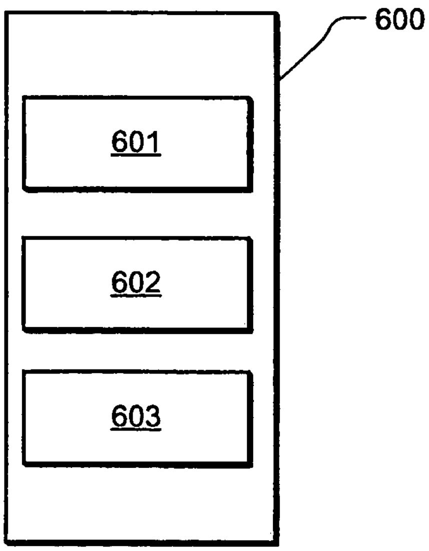


Fig. 7

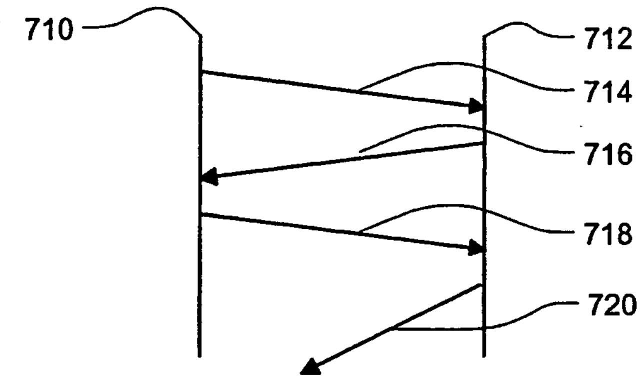


Fig. 8

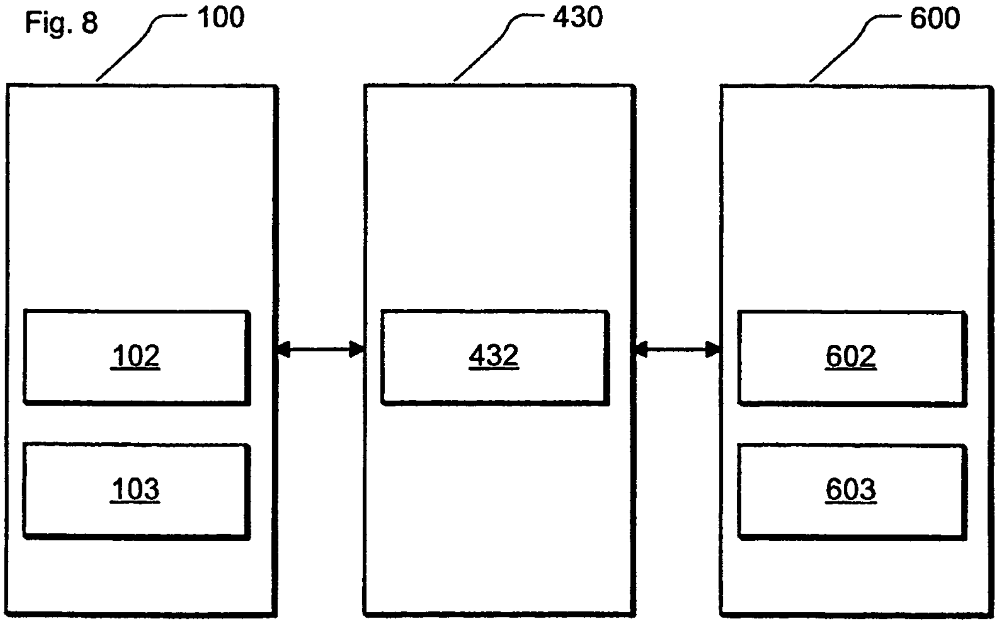
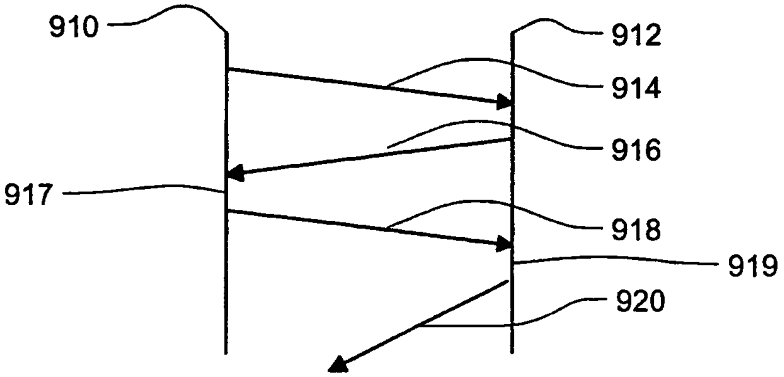


Fig. 9



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/13444

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04L 9/02
US CL :713/155, 168, 172, 201
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/155, 168, 172, 201

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WEST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,091,942 A (DENT) 25 February 1992, col. 10, lines 31-40; col. 13, line 66 to col. 14, line 22; col. 16, line 67 to col. 17, line 6 and col. 17, line 56 to col. 18, line 7.	1-59
Y	US 5,875,394 A (DALY et al) 23 February 1999, col. 3, line 53 to col. 4, line 51.	11-17, 24-30, and 37-40,
Y	US 5,974,312 A (HAYES et al) 26 October 1999, col. 5, lines 61-67; col. 10, line 3 to col. 16, line 34.	1-59

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance		
"E"	earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search 26 JUNE 2001	Date of mailing of the international search report 02 AUG 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer MATTHEW SMITH James R. Matthews Telephone No. (703) 308-9293